Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 5 | May 2017

STUDY ON RANSOMWARE ATTACK AND ITS PREVENTION

Ganesh Gupta [1] | Dr. Khushboo Tripathi [1]

[1] Assistant Professor, ASET, Amity University Haryana ,Gurugram (Manesar), India - 122413.

ABSTRACT

Ransomware is a serious and growing cyber security issue. It has potential to inflict serious financial harm on an organization while damaging reputation and utility. Due to this attack daily 4000 average number of individuals are affected only in United States. Medical practices are a prime target for this attack because of the quantity and value of their data. The objective of this paper is to create awareness among less skilled computer users by providing cyber safeguard knowledge and regular updating practice of prevention techniques.

KEYWORDS: Ransomware, Bitcoin, CryptoWall, CryptoViral, Zeroizes.

INTRODUCTION

Ransomware is a type of malware (malicious software). Its defining characteristic: ransomware attempts to deny access to a user's (or organization's) data, usually by encrypting the data with a key known only to the cybercriminal who deployed the malware. After the data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a digital currency such as Bitcoin) in order to receive a decryption key. The amount of ransom requested typically increases, if the cybercriminal determines the data has substantial value.

The medical practice was hit by Crypto locker, a type of ransomware virus. It rendered the practice inoperable for several days, and crippled its technology for more than a week. The attack made its way onto one of the practice's computers via an email attachment, which had the appearance of a vendor invoice.

Once on a computer, it searched for files to encrypt. This included files on the computer itself as well as those on the practice's network that were accessible via mapped network drives. Files on any drive letter or network share that could be located and accessed (with a program such as Windows Explorer) was accessed by the ransomware.

The practice immediately went to paper for scheduling, clinic notes and prescriptions. The practice's IT department downloaded all of its backup data and then uploaded it to its server to replace the corrupted data. The entire process took several days as the backup data was stored offsite, which required transportation of the data; the data needed to be cleaned with antivirus software; and then settings and policies needed to be recreated [3].

Attackers employ various tactics to help them effectively spread ransomware through spam emails. For example some attacker used Window Script Files(WSF) to bypass email filtering. Files with .wsf extension cab be launched like an executable file. Once the email attachment folder appearing to contain a .doc file is opened, the .wsf file is executed and CryptoWall is installed in victim's computer.

As seen that ransomware composed entirely of JavaScript, Which was being spread through spam attachments posting as .doc files. Once the malicious attachment was opened, JS.Racryptor, also known as RAA, immediately began encrypting files. JavaScript was used as a framework for developing desktop applications for Windows, Linux, and Mac OS X using JavaScript. However, while ransomware was packed into executable file, was delivered solely by a JavaScript file.

How it Works:

A large scale cyber attack was launched affecting tens thousands of computer systems in over 100 countries around the globe. The process of attacker and victim ransomware are in given following steps:

Step1: The attacker generates a key pair and places the corresponding public key in the malware. The malware is released.

Step2: To carry out the cryptoviral extortion attack, the malware generates a random symmetric key and encrypts the victim's data with it. It uses the public key in the malware to encrypt the symmetric key. This is known as hybrid encryption and it results in a small asymmetric ciphertext as well as the symmetric ciphertext of the victim's data. It zeroizes the symmetric key and the original plaintext data to prevent recovery. It puts up a message to the user that includes the asymmetric ciphertext and how to pay the ransom. The victim sends the asymmetric ciphertext and e-money to the attacker.

Step3: The attacker receives the payment, deciphers the asymmetric ciphertext with the attacker's private key, and sends the symmetric key to the victim. The victim deciphers the encrypted data with the needed symmetric key thereby completing the cryptovirology attack.

The symmetric key is randomly generated and will not assist other victims. At no point is the attacker's private key exposed to victims and the victim need only send a very small ciphertext (the encrypted symmetric-cipher key) to the attacker.

Ransomware attacks are typically carried out using a trojan, entering a system through a downloaded file or a vulnerability in a network service[1][2].

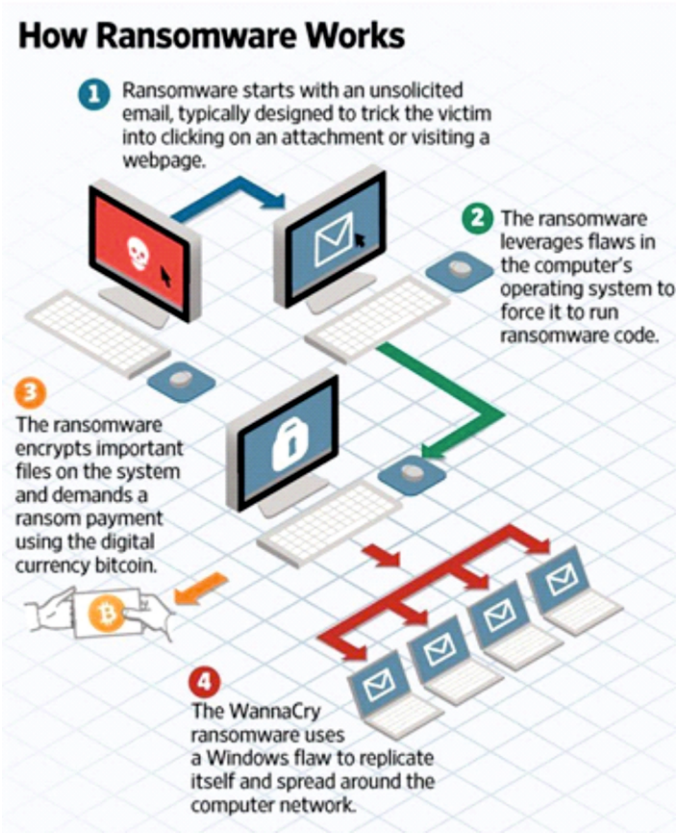

Figure 1 : Working of Ransomware[7]

Impacts of the Attack:

The potential impacts that an organization could face after a ransomware attack include the following:

- **Shutdown Cost:** Organization may be forced to shut down systems to deal with the infection. Customers may be affected as the targeted organization's services may be impacted. Because of the downtime, the company could experience reputational damage.

- **Data or Information loss:** Loss of data due to files being encrypted and stolen can have a huge impact on businesses. The loss of company records, customers personally identifiable information, or intellectual property can significantly impact the organization. The cybercriminals behind the attack may threaten to publish stolen data online in an attempt to extort more money from victim.

- **Financial Cost:** Companies may have to pay for the incident response and other security related solutions in response to ransomware. Organizations could also be hit with large legal bills if customers are affected. Fines and other penalties may also apply.

- **Loss of life:** In the case of a hospital or other medical organization, patients lives may put at risk as essential medical equipment may be affected. Patient record including medical history may be inaccessible, leading to delays in treatment or even incorrect medication.

How to prevent:

Preventing infection is by far best outcome so adopting a robust defensive against these infection vectors will help us to reduce the risk of infection.

1. **Email Security:** Email-filtering services such as Symantec Email Security, cloud can help to stop malicious emails before they reach users. Symantec Messaging Gateway's technology can also protect computers from this threat by removing malicious content from attached document before they even reach the user.

   Email.cloud technology includes Real Time Link Following (RTLF) which process URLs present in attachments, not just in the body of emails. In addition to this, Email.cloud has advanced capability to detect the block malicious JavaScript contained within emails through code analysis and emulation.

2. **Intrusion Prevention:** Different intrusion prevention system (IPS) technology can detect and block malicious traffic from exploit kit activity, preventing the installation of ransomware.

3. **Download Insight:** Many Download Insight technology examines files that are downloaded through or launched by web browsers, messaging clients, and other portals. Download Insight determines whether a file is a risk based on reputation.

4. **Browser Protection:** Secure Browser Protection solution analyzes the web browser's state and blocks websites from delivering exploits.

5. **Exploit Protection:** Symantec exploit protection technology recognizes a range of malicious behaviors that are common in exploit attacks and blocks them from executing.

6. **Best Practice:** End users are advised to immediately delete any suspicious emails they receive, especially those containing links and/or attachments. Be wary of Microsoft Office attachments that prompt users to enable macros. While macros can be used for legitimate purposes, such as automating tasks, attackers often use malicious macros to deliver malware through Office documents. To mitigate this infection vector, Microsoft has disabled macros from loading in Office documents by default. Attackers may use social-engineering techniques to convince users to enable macros to run. As a result, Security tool recommends that user should avoid enabling macros in Microsoft Office.

CONCLUSION

Anti-ransomware security tools may be a reliable solution, However some paid antivirus product includes an automatic update module and a real-time scanner. We must understand the importance of having a traffic-filtering solution that can provide proactive anti-ransomware protection.

REFERENCES

1. Gregg Keizer ,G.(2011): Ransomware squeezes users with bogus Windows activation demand,available at http:// www. computerworld.com/ , accessed 18 May 2017.
2. Robert. McMillian, R.(2010): Alleged Ransomware Gang Investigated by Moscow Police, available at http:// www.pcworld.com/article/204577/article.html, accessed on 21 May 2017.
3. Wiks Moffat : Ransomeware Attack On a medical Practice: A Case Study With Guidance, available at https:// www. conventusnj.com/practice-resources/ regulatory/ransomware-attack-medical-practice-case-study.aspx , accessed 18 may 2017
4. Siddharth Ghansela, "Network Security: Attacks, Tools and Techniques", International Journal of Advanced Research in Computer Science and Software Engineering , Vol 3(6), pp. 419-421, June-2013.
5. Neelam Janak Kumar Patel, Khushboo Tripathi, "Detection & Prevention Techniques of Sybil Attack& its Analysis in Mobile Adhoc Network", Vol. 5, Issue 7, pp. 12287 - 12297 ,July 2016.
6. Songmei Zhang, Shan Yao, Xin'en Ye, Chunhe Xia, "A Network Security Situation Analysis Framework Based on Information Fusion", IEEE , pp. 326-332, 2011.
7. Gary Baker, G.(2017):U.K's Healthcare System Victim of Vicious Global Cyberattack, available at: https://www.xmedius.com/en/u-k-s-healthcare-system-victim-of-vicious-global-cyberattack/ , accessed 17 may 2017.